

# Cancer Prevention and Research Institute of Texas

IA #02-2020 Disaster Recovery and Business Continuity

Planning Advisory Audit Report

Report Date: September 29, 2020

Issued: October 28, 2020

# CONTENTS

	Page
Audit Advisory Report Transmittal Letter to the Oversight Committee.....	1
Background.....	2
Audit Scope and Objectives.....	3
Executive Summary.....	4
Conclusion.....	5
Detailed Procedures Performed, Results, Recommendations and Management Response .....	6
Objective A: DR/BC Planning Evaluation.....	7
Objective B: Recommendations for Improvement.....	8



The Oversight Committee  
Cancer Prevention and Research Institute of Texas  
1701 North Congress Avenue, Suite 6-127  
Austin, Texas 78701

This report presents the results of the audit advisory procedures performed for the Cancer Prevention and Research Institute of Texas (CPRIT or 'the Institute') during the period July 15, 2020, through September 28, 2020, relating to the Disaster Recovery and Business Continuity Plans (DR/BC plans) developed by CPRIT.

The objectives of the audit advisory procedures were to evaluate the design and effectiveness of the Institute's DR/BC planning preparation for emergency situations. The objectives were organized as follows:

- Evaluate CPRIT's DR/BC planning against existing regulatory requirements and the risks inherent to the planned processes.
- Provide CPRIT with recommendations to strengthen the Institute's DR/BC planning and improve risk management consistent with required and authoritative best practice criteria.

To accomplish these objectives, we conducted interviews with CPRIT personnel responsible for the disaster recovery and business continuity functions and examined existing documentation to gain an understanding of current DR/BC planning processes and procedures. With consideration to the health and safety precautions necessary for the COVID-19 pandemic, procedures were performed remotely and completed on September 29, 2020.

The following report summarizes the results of our procedures, our recommendations for improvement and CPRIT management responses.

*Weaver and Tidwell, L.L.P.*

WEAVER AND TIDWELL, L.L.P.

Austin, Texas  
October 28, 2020

Weaver and Tidwell, L.L.P.  
1601 South MoPac Expressway, Suite D250 / Austin, Texas 78746  
Main: 512.609.1900

**CPAs AND ADVISORS | WEAVER.COM**

# Cancer Prevention and Research Institute of Texas

## IA #02-2020 Disaster Recovery and Business Continuity Planning Advisory Audit Report

September 29, 2020  
Issued: October 28, 2020

### Background

CPRIT’s mission is to expedite discoveries and innovations across Texas to reduce the burdens of cancer. CPRIT’s Oversight Committee awarded its first cancer research grant in late 2009. Eleven years later, CPRIT has invested over \$2.6 billion – 95 percent of the original \$3 billion of funding approved by Texans for grant awards – in 1,576 grants. When Proposition 6 passed on November 5, 2019, CPRIT became a \$6 billion, 20-year initiative. Of the \$2.6 billion awarded as of August 31, 2020, 10 percent of CPRIT’s funding (244 grants) supports cancer prevention efforts throughout the state. The other 90 percent of CPRIT’s funding supports the academic and product development research award portfolio (1,332 grants) which includes projects spanning the research and development continuum from basic through clinical research. As of August 2020, CPRIT is administering 550+ active grants totaling \$1.4 billion.

The work of coordinating grant application receipt and review, awarding and monitoring grants, and administering required state agency functions is performed by a small agency staff of 36 full-time equivalents from an office located in Austin, Texas. Due to the small number of staff, CPRIT uses service contracts strategically to augment the staff size and enhance the capabilities necessary to perform this work. CPRIT’s IT infrastructure is distributed in systems that facilitate sharing data with various contractors and grantees, and enable continued operations and ongoing accessibility to data for staff, including supporting a remote working environment.

The Institute has developed DR/BC plans to prepare for and respond to disruptive events. A disruptive event is recognized as causing an entity’s information and communications systems to be inaccessible or disabled and inhibiting business operations. In some instances, a disruptive event may be dangerous or even life-threatening to staff.

- Disaster Recovery (DR) planning includes an entity’s actions in preparing for, responding to and resolving a critically disruptive event. The focus of a DR plan is the recovery of an entity’s IT systems, applications and data when a disruptive event occurs.
- Business Continuity (BC) planning embodies a more holistic approach concerning the continuity of an entity’s operations according to established contingency measures taken to address pre-determined thresholds. Disaster recovery is considered a component of business continuity planning. While a DR plan is focused on the recovery of IT systems and data, the BC plan focuses on restoring and resuming operations for the entity as a whole.

State agencies must adhere to the following standards in the development and maintenance of their DR/BC plans:

Author	Standard	Description
State Office of Risk Management (SORM)	Texas Continuity Template and Toolbox.	Provides a blueprint for the structure and content of agency DR/BC plans.
Texas Department of Information Resources (DIR)	Security Control Standards Catalog	Specifies the minimum information security requirements that state organizations must use to provide the appropriate levels of information security according to risk levels.

# Cancer Prevention and Research Institute of Texas

## IA #02-2020 Disaster Recovery and Business Continuity Planning Advisory Audit Report September 29, 2020 Issued: October 28, 2020

Additionally, the National Institute of Standards and Technology (NIST) Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* was utilized as an authoritative source for instructions, recommendations and considerations when evaluating CPRIT's DR/BC planning documents.

CPRIT's most current DR/BC planning documents are dated April 2020. These documents are maintained and revised as needed (reviewed annually at a minimum) by the Reconstitution Planning Team, overseen by the CEO.

### **Audit Scope & Objectives**

This audit advisory project focused on CPRIT's Disaster Recovery and Business Continuity (DR/BC) planning documents. We reviewed the processes and procedures outlined in these documents for compliance with regulatory requirements and appropriate risk management coverage. Our scope included an evaluation of the processes and procedures that cover the activities in the following key areas:

#### **Disaster Recovery Activities:**

- Disaster Recovery Plan and Procedures
- IT Backup and Recovery Systems
- IT Hardware Recovery
- Data Recovery
- Disaster Recovery Testing

#### **Business Continuity Planning Activities:**

- Business Resumption Plan and Procedures
- Scenario Determination and Criticality
- Business Impact Analysis
- Business Resumption
- Continuity Plan Testing

Our procedures were designed to evaluate CPRIT's DR/BC plans and provide recommendations for improving the plans and enhance risk management processes, in alignment with regulatory standards and authoritative best practices guidance.

The objectives of the audit advisory procedures were to evaluate the design and effectiveness of the Institute's DR/BC planning for emergency situations. The objectives were organized as follows:

- Evaluate CPRIT's DR/BC planning against existing regulatory requirements and the risks inherent to the planned processes.
- Provide CPRIT with recommendations to strengthen the Institute's DR/BC planning and improve risk management consistent with required and authoritative best practice criteria.

**Cancer Prevention and Research Institute of Texas**  
 IA #02-2020 Disaster Recovery and Business Continuity Planning Advisory  
 Audit Report  
 September 29, 2020  
 Issued: October 28, 2020

Our procedures included interviews with CPRIT personnel responsible for the disaster recovery and business continuity functions and examination of existing documentation to gain an understanding of current DR/BC planning processes and procedures. We evaluated the processes and procedures outlined in the draft DR/BC plans in their current state.

**Executive Summary**

As part of our evaluation, we mapped the DR/BC planning criteria required by the State Office of Risk Management (SORM) and the Texas Department of Information Resources (DIR), as well as the guidance provided by the National Institute of Standards and Technology (NIST) to the DR/BC planning procedures and processes outlined in the drafts of CPRIT DR/BC documents that include:

- Continuity of Operations Plan (COOP),
- Reconstitution Plan,
- Information Technology Disaster Recovery Plan, and
- 10 other DR/BC planningP related supporting documents

Through our interviews with CPRIT personnel and our evaluation of CPRIT’s DR/BC planning documentation, we identified 30 separate recommendations to improve the draft DR/BC plans. We provided the recommendations including proposed revisions to the planning documents to the personnel responsible for DR/BC planning for their evaluation.

The recommendations identified are intended to assist CPRIT in strengthening the existing procedures and processes used to respond to a disruptive event and further mitigate potential financial, operational and regulatory risks when responding to such an event.

A summary of our results, by objective is provided below.

SCOPE AREA	RESULT
<p><b>Objective A:</b>            Evaluate CPRIT’s DR/BC planning against existing regulatory requirements and the risks inherent to the planned processes.</p>	<p>CPRIT’s draft DR/BC planning documents are generally consistent with required and authoritative best practice criteria. Of the 121 separate required and best practice criteria elements that should be included in the DR/BC planning documents, we identified 30 recommendations to improve and better align CPRIT’s planned processes and procedures with these elements. These recommendations include:</p> <ul style="list-style-type: none"> <li>• 24 to augment or revise information related to required criteria</li> <li>• 6 to improve general clarity and better align the planning documents</li> </ul>

**Cancer Prevention and Research Institute of Texas**  
 IA #02-2020 Disaster Recovery and Business Continuity Planning Advisory  
 Audit Report  
 September 29, 2020  
 Issued: October 28, 2020

SCOPE AREA	RESULT
<p><b>Objective B:</b>            Provide CPRIT recommendations to strengthen the Institute’s DR/BC planning and improve risk management consistent with required and authoritative best practice criteria.</p>	<p>Based on the 30 recommendations identified in Objective A, we provided detailed feedback to CPRIT personnel to update, revise, or clarify the existing DR/BC planning documents. Specifically, we provided:</p> <ul style="list-style-type: none"> <li>• 23 draft revisions to augment or update the existing documentation</li> <li>• 7 recommendations for updates to technical information for IT platforms in the planning documentation</li> </ul>

**Conclusion:**

Based on our evaluation, the Institute has adequate DR/BC planning documents that incorporate a significant portion of the criteria defined by the State Office of Risk Management and the Texas Department of Information Resources. However, we identified opportunities to augment and clarify the information in the documentation to improve compliance with regulatory criteria and the risk management posture of the agency.

Management should review and evaluate the proposed edits to strengthen the DR/BC planning documents. Once the modifications have been adopted and the Institute’s DR/BC plans are finalized, we recommend that Management develop a plan and schedule for testing the DR/BC plans processes and procedures.

**Detailed Procedures Performed, Results,  
Recommendations and Management  
Response**

**Cancer Prevention and Research Institute of Texas**  
 IA #02-2020 Disaster Recovery and Business Continuity Planning Advisory  
 Audit Report  
 September 29, 2020  
 Issued: October 28, 2020

**Objective A: DR/BC Planning Evaluation**

Evaluate CPRIT's DR/BC planning against existing regulatory requirements and the risks inherent to the planned processes.

**Procedure performed:**

We obtained and compared the drafts of CPRIT's DR/BC planning documentation against a criteria matrix that included both required and authoritative best practice criteria elements. CPRIT's DR/BC planning documentation and the authoritative materials used in this comparison, include:

CPRIT DR/BC Planning Documentation	Authoritative Criteria & Guidance
1. Continuity of Operations Plan [DRAFT] 2. Reconstitution Plan [DRAFT] 3. IT Disaster Recovery Plan 4. Employee Assistant Program 5. Safety and Occupational Health Manual 6. Emergency Response Team 7. Data Repository Log 8. IT DR Service Listing 9. IT DR Executive Briefing/Recovery Prioritization Review 10. IT Disaster Recovery Service Catalog 11. IT Contacts listing 12. On-site Hardware Requirements 13. Disaster Recovery Simulation Test Report	1. State Office of Risk Management (SORM) - <i>Texas Continuity Template and Toolbox</i> . 2. Texas Department of Information Resources (DIR) - <i>Security Control Standards Catalog</i> . 3. National Institute of Standards and Technology (NIST) - <i>Special Publication (SP) 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems</i> .

**Results:**

We identified 30 opportunities to improve CPRIT's DR/BC planning documents with relation to the 121 required and authoritative best practice criteria throughout various DR/BC planning components.

DR/BC Component	Total Criteria	Improvement Opportunity		Nature of Improvement Opportunity		
		Count	Type	Content Addition	Content Revision	Reference Update
Incident Evaluation	31	8	R	5	2	1
		1	OA	1	-	-
Incident Management	30	10	R	3	4	3
		1	OA	1	-	-
Disaster Recovery	37	1	R	1	-	-
		-	OA	-	-	-
Business Resumption	23	5	R	4	-	1
		4	OA	2	2	-
<b>Total</b>	<b>121</b>	<b>30</b>		<b>17</b>	<b>8</b>	<b>5</b>

**R - Required elements by SORM or DIR**

**OA - Other authoritative guidance**

# Cancer Prevention and Research Institute of Texas

## IA #02-2020 Disaster Recovery and Business Continuity Planning Advisory Audit Report September 29, 2020 Issued: October 28, 2020

The recommendations comprise proposed edits to specific information within the DR/BC planning documentation that augments existing content, revisions to content for clarity, and updates to references to other documents among the suite of DR/BC planning documents intended to reduce the effort by CPRIT personnel to maintain and keep the documentation up-to-date and relevant. These recommendations include:

- First responder/incident evaluation team references
- Additional incident scenario descriptions for fire and hacking/ransomware
- Documenting business impacts relating to IT data application losses
- Strengthening media inquiry routing protocols
- Identifying dependencies for essential functions
- Further defining funding sources for recovery activities
- Documenting identified vendors for IT assessment and restoration services
- Documenting initial and final server configurations
- Access to and closure of emergency purchase ordering
- Asset removal/disposal process

### **Objective B: Recommendations for Improvement**

Provide CPRIT recommendations to strengthen the Institute's DR/BC planning and improve risk management consistent with regulatory and authoritative best practice criteria.

#### **Procedure performed:**

Based on the opportunities for improvement identified in Objective A, we closely collaborated with CPRIT personnel responsible for different DR/BC planning components to develop and craft appropriate edits to the existing documentation. We conducted meetings where we discussed possible revisions to the existing documentation in detail with CPRIT personnel to confirm the purpose and content of the edits prior to drafting the proposed revisions for CPRIT's use.

#### **Results:**

We drafted revisions for 23 of the 30 recommendations and provided them to CPRIT. The proposed edits include updates to CPRIT's Continuity of Operations Plan, Reconstitution Plan, and Information Technology Disaster Recovery Plan.

We also provided seven recommendations for modifications to technical content related to IT platform system information and configurations contained in the DR/BC planning documentation. These modifications to technical content would improve the clarity of the DR/BC planning documentation if CPRIT IT personnel were unavailable during a disaster event or crisis scenario.

#### **Recommendation:**

Management should review proposed revisions to the DR/BC planning documentation, modify as appropriate and finalize the DR/BC plans. Upon finalization, CPRIT should test the plans and develop and implement a strategy to review and update the documentation periodically based on changes in CPRIT's IT infrastructure or operations as well as conduct periodic testing of the plans.

# Cancer Prevention and Research Institute of Texas

IA #02-2020 Disaster Recovery and Business Continuity Planning Advisory

Audit Report

September 29, 2020

Issued: October 28, 2020

**Management Response:** Management appreciates the time that Weaver personnel took in reviewing CPRIT's DR/BC planning documentation, conducting meetings with CPRIT personnel to ask questions about the documentation as well as respond to CPRIT's questions, and providing draft language for revisions to clarify or enhance the documentation. This assessment of the DR/BC planning documentation has been invaluable to the agency's disaster response preparedness. The suggested revisions and draft language will be incorporated appropriately in the DR/BC planning documentation. After the documentation has been updated, CPRIT will schedule tests of the plans and conduct after action evaluations to determine whether additional modifications need to be made to the processes and procedures in the planning documents.

**Responsible Party:** Chief Operating Officer, Operations Manager, IT Manager

**Implementation Date:** June 30, 2021